

**AUTHENTICATION AND AUTHORIZATION PROTOCOL FOR SECURE  
WEB-BASED ACCESS TO A PROTECTED RESOURCE**

**ABSTRACT OF THE DISCLOSURE**

5           When a user makes a request to access a protected  
resource identified by a URL, client-side code in a web  
browser is used to generate an authentication token,  
which is then sent to the server along with an identity  
cookie that was set by that server. The authenticated  
10 token is then used by the server to authenticate that the  
request is properly tied to a given identity contained in  
the identity cookie. If the authentication token can be  
validated at the server, an access control decision is  
then executed to determine whether to invoke the request  
15 for the protected resource. If the authentication token  
cannot be validated, an access denied request is returned  
to the requesting client.